FIG. **3**B. If so, at Block **340**, independent authentication may be obtained from the user **160'** by, for example, asking the user **160'** to show a picture identification or to provide and/or participate in some other independent authentication prior to approving the transaction. It will be understood that the user **160'** may be authorized even though the single wireless terminal **150'** is not proximate to the user **160'** because the user's spouse or child may be using the single wireless terminal **150'** at the time of the prospective credit card transaction, or the user **160'** may have accidentally left the single wireless terminal **150'** at another location, such as at home. Nonetheless, due to the heightened possibility of fraud, additional authentication may be obtained at Block **340**.

[0048] Returning again to Block **310**, if the wireless network interface **114** determines that multiple wireless terminals, such as wireless terminals **150'** and **150"**, are associated with the user **160'** of the credit card **162'** for the prospective credit card transaction at the credit card transaction terminal **130'**, then a test is made at Block **350** as to whether all of the multiple wireless terminals that are associated with the user **160'** are sufficiently close to the credit card transaction terminal **130'**, for example located within the distance **300**. If this is the case, then the transaction may be authorized at Block **330**. Thus, in some embodiments of the invention, a given user **160'** may carry two cell phones, a cell phone and a personal digital assistant, a cell phone and a pager, etc. If they are all close to the transaction terminal **130'**, it is highly likely that they are all being carried by the user **160'** and additional authentication may not be needed.

[0049] Returning again to Block **350**, if all of the wireless terminals **150'**, **150"** are not located near the transaction terminal **130'**, a test is made at Block **370** as to whether different wireless network providers **140** provide the different wireless terminals **150'**, **150"**. For example, an inquiry may be made as to whether the first wireless terminal **150'** and the second wireless terminal **150"** are provided by different wireless network providers **140**. If this is the case, then at Block **390**, additional authentication may be required of the user, whereas, at Block **380**, if the same network provider **140** provides the different terminals **150'**, **150"**, a lower level of authentication may be obtained from the user at Block **380**.

[0050] Embodiments of Blocks **370**, **380** and **390** may arise from recognition that a thief may attempt to spoof location based credit card authorization by registering an additional wireless terminal in the user's name, so that the additional wireless terminal is proximate the fraudulently obtained credit when a thief attempts to use the fraudulently obtained credit card. However, in these circumstances, it may be difficult for the thief to obtain a new terminal from the same wireless network provider as the legitimate user's wireless terminal. For instance, for reasons of marketing/security/billing, the same wireless provider may question and/or investigate multiple registration attempts and/or even contact the legitimate user. Thus, the thief may try to obtain a second wireless terminal from a different wireless network provider. Accordingly, a heightened level of authentication may be required at Block **390** when different wireless network providers provide the multiple wireless terminals **150'**, **150"**, compared to when all of the wireless terminals were obtained from the same wireless network provider. It will also be understood that there may be circumstances where the different wireless network terminals may have been obtained from different wireless network providers by a legitimate user. For example, a user may have a home cell phone from one wireless network provider and a business cell phone from another wireless network provider. Nonetheless, to reduce the likelihood of fraud, additional authentication may be obtained at Block **390** when different wireless network providers are present at Block **370**.

[0051] Embodiments of FIGS. **3**A and **3**B have referred to one or more wireless terminals **150'**, **150"** that are associated with a user **160'** of a credit card **162'** for the prospective credit card transaction being "sufficiently close" or "near" the credit card transaction terminal **130'**. The definition of "sufficiently close" or "near" may always be the same or may vary depending upon the application. For example, it may required that the wireless terminal **150'** is within 10 feet, or a minimum resolution distance of the location determining system, of the credit card transaction terminal **130'**, to ensure that the wireless terminal **150'** is actually carried on the person of the user **160'**. However, this distance **300** may be relaxed by a given credit card issuer and/or merchant. For example, in retail stores where a checkout line is used, the user **160'** of the credit card **162'** is generally very close to the credit card transaction terminal **130'**. However, in a department store or other store that does not use checkout lines, the credit card transaction terminal **130'** may be located a considerable distance away from the user, so that the distance **300** therebetween may be set to be larger, for example, up to about 30 feet. In other retail environments, the user **160** may actually browse the store while the transaction is being authorized, so that even greater distances **300** may be permitted. In still other embodiments, the acceptable distance **300** may be based on the type of wireless terminal **150'**. For example, a laptop computer may be kept in a briefcase, and may be allowed a wider latitude than a cell phone or pager which is typically carried by the user. Moreover, the distance **300** may vary based on the time of day, the occurrence of certain sales or promotions, the history of use, types/models of wireless terminal, types/models of merchant terminal, ambient wireless interference conditions, error conditions and/or thresholds, the number of wireless devices registered to the user and/or other criteria, or may be fixed.

[0052] Moreover, the authentication levels that are described in Blocks **340**, **380** and **390** may vary based on the identity of the merchant, the amount of the credit card purchase, the history of the user or the merchant and/or other known parameters. The authentication level obtained in Blocks **340** and **380** may be same or may be different. The additional authentication that is obtained in Block **390** is a higher level of authentication than Block **380**. Various levels of authentication for credit card transactions are well known to those having skill in the art and may include providing an independent picture identification, providing one or more password/pass code/PIN (Personal Identification Number), providing secret information or answers to questions known only to the user over a phone line or other communication medium, an extended conversation with the representative of the credit card issuer and/or the merchant, and many other levels of authentication well known to those having skill in the art. Additional discussion of authentication levels will be provided below.

[0053] FIG. **4** is a flowchart of operations that may be performed to correlate the locations of the credit card transaction terminal **130** that is associated with the prospective credit card transaction and one or more user wireless terminals **150** that are associated with the user **160** of the credit card **162**, according to various embodiments of the present inven-